TASK ORDER

GSQ0017AJ0079 PO13

Secure Enterprise Network Systems, Services, & Support (SENS3)

in support of:

Department of Homeland Security (DHS) Information Technology Services Office (ITSO)

Issued to:
Leidos Innovations Corporation

Awarded under GSA Alliant Government-wide
Acquisition Contract GS00Q09BGD0039

Conducted under Federal Acquisition Regulation (FAR) 16.505

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

August 31, 2017

FEDSIM Project Number: HS00800

C.1 BACKGROUND

C.1.1 PURPOSE

The Department of Homeland Security's (DHS) Information Technology Services Office (ITSO) and Office of Intelligence & Analysis (I&A) have a requirement for Secure Enterprise Network Systems, Services, & Support (SENS3) to address the mission-critical need for DHS to maintain and manage effective secure classified information sharing and safeguarding of classified information among all DHS Components, its Federal, state, local, and tribal partners, and stakeholders in support of its classified enterprise operations. The DHS mission is dependent on a secure, reliable, and capable classified information sharing infrastructure that is interoperable across DHS and partner classified environments. These environments consist of the Homeland Secure Data Network (HSDN), the C-LAN, and supporting systems and interfaces, as well as cross domain guards connecting the DHS unclassified networks with HSDN and C-LAN networks. DHS was specifically directed to address these requirements through multiple legislative actions and executive orders including, but not limited to: the Homeland Security Act of 2002, as amended; the Implementing the Recommendations of the 9-11 Commission Act of 2007, Executive Order (EO) 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans;" and EO 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."

The HSDN is the Secret-level, civilian classified network with connectivity to the Defense Information System Agency (DISA) provisioned Secret Internet Protocol Router Network (SIPRNet). The C-LAN provides similar services at the Top Secret/Sensitive Compartmented Information (TS/SCI) level with connectivity to the Defense Intelligence Agency (DIA)-provisioned Joint Worldwide Intelligence Communications System (JWICS). These DHS classified networks provide a Federal enterprise infrastructure for classified information sharing that extends existing United States (U.S.) Government capabilities not only to DHS, but to other Federal Government agencies and to first responders at the state, local, and tribal levels.

The continued evolution of the HSDN and the C-LAN will leverage advancements in technology to enhance or replace existing network components with newer, better maintained technologies to avoid performance degradation and obsolescence. This continual service improvement includes the formulation and the execution of alternative approaches and architectures for optimizing and modernizing the HSDN and the C-LAN networking environments, including managed service models and available cloud technologies.

C.1.2 AGENCY MISSION

DHS is a widely distributed and diverse national enterprise. The vision of homeland security is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards. These concepts have led DHS to define its core mission set as:

a. Preventing Terrorism and Enhancing Security,

b. Securing and Managing Our Borders,

c. Enforcing and Administering Our Immigration Laws,

d. Safeguarding and Securing Cyberspace,

e. Ensuring Resilience to Disasters.

C.2 SCOPE

The scope of SENS3 addresses the operations and maintenance, security, optimization, enhancement, design, engineering, architecture, integration, configuration, testing, and deployment of the DHS HSDN and C-LAN networks, infrastructure (including hardware and software), cross domain services operating on DHS unclassified, HSDN and C-LAN networks, and other systems supporting the intelligence mission collectively referred to as the SENS3 networks (see Section J, Attachment E – Functional Requirements).

C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

The network infrastructure environment managed by DHS is used to deliver secure enterprise network systems and services. When the Department was stood up in 2003, the infrastructure it inherited comprised dozens of networks that had earlier been developed and managed independently by the previously separate agencies. Under "One DHS" policies, the DHS Office of the Chief Information Officer (OCIO) has been merging and harmonizing existing networks into offerings that will provide effective and efficient network services, while saving considerable costs through a common architecture, shared management, and leveraged investments. Central to the infrastructure transformation program is the separate OneNet initiative. OneNet comprises network circuit provisioning orders established under the GSA Networx program to supply DHS with its communications connectivity. DHS currently operates one unclassified network (A-LAN) and two secure, classified networks, HSDN which operates at the Secret level and C-LAN which operates at the TS/SCI level. HSDN and the C-LAN provide a common core of essential services (e.g., Service Desk, Network Operations Center (NOC), cross-domain services, servers, and virtual machines) and the associated infrastructure, which are necessary to operate and maintain the IT environments for all users. SENS3 also includes support for other systems supporting the intelligence mission (see Section J, Attachment E – Functional Requirements).

The HSDN is a fully operational Government-wide infrastructure solution managed by DHS, designed and implemented to provide standardized, secure transport with desktop applications to enable a consistent classified capability in support of the DHS mission. HSDN is deployed to more than 700 locations across the continental U.S. including many locations at other Federal agencies and over 40 SLFCs (see Section J, Attachment FF – HSDN and C-LAN Site Deployment Map). It is isolated from the Internet with no public access. HSDN has approval to operate in accordance with DHS Policy 4300B, which is based upon Committee on National Security Systems instruction (CNSSI) 1253, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 (Guide for Applying the Risk Management Framework to Federal Information Systems) and NIST SP 800-53A (Guide for Assessing the Security and Privacy Controls in Federal Information Systems and Organizations) security standards. HSDN consists of two sets of fully redundant core infrastructures of routers, servers, and data storage located at the two DHS Data Centers (DC1 and DC2) and connected by DHS' wide area network (OneNet) that carries only classified network traffic in an encrypted state. It also includes two redundant gateways connecting HSDN as a peer to other Secret networks (e.g., the Department of Defense (DoD) Secret Internet Protocol Router Network (SIPRNet)), a NOC, Public Key Infrastructure (PKI), and a service desk. The HSDN core infrastructure connects to end-user sites via DHS OneNet as a backbone network. Networked components at those nodes include end point routers, encryptors, thick clients, thin clients, printers, Secure Video Teleconferencing (SVTC) clients, and voice over secure internet protocol (VoSIP) clients. Services hosted on the HSDN core infrastructure include electronic mail (email), organizational messaging (e.g., the Automated Message Handling System (AMHS)), SVTC connection and bridging, a web portal, collaboration tools, application hosting services, global backup and recovery services, and standard office productivity tools. The HSDN core infrastructure connects to handheld devices for secret-level voice capability through a mobile architecture accepted by the Commercial Solutions for Classified (CSfC) Program. HSDN offers several standard end-point configurations including handheld devices, laptops, small sites, medium sites, and large custom sites.

C-LAN is a fully operational DHS enterprise-wide infrastructure solution designed and implemented to provide standardized, secure transport with desktop applications to enable a consistent TS/SCI capability in support of the DHS mission. C-LAN is deployed to more than 50 locations across the continental U.S. including state and local partners (see Section J, Attachment FF – HSDN and C-LAN Site Deployment Map). It is isolated from the Internet with no public access. C-LAN has approval to operate in accordance with DHS Policy 4300C. C-LAN consists of two sets of fully redundant core infrastructures of routers, servers, and data storage located at DC1 and DC2 and connected by DHS' wide area network (OneNet). C-LAN provides a NOC, a Voice/Video Operations Center (VVOC), and a service desk as an enclave of JWICS. The C-LAN core infrastructure connects to end-user sites via DHS OneNet as a backbone network. Networked components at those nodes include end point routers, encryptors, thick clients, thin clients, printers, SVTC clients, and VoSIP clients. Services hosted on the C-LAN core infrastructure include electronic mail (email), organizational messaging (e.g., AMHS), SVTC connection and bridging, a web portal, collaboration tools, application hosting services, global backup and recovery services, and standard office productivity tools.

C.4 OBJECTIVES

The objectives for SENS3 represent the desired outcomes of the support services being sought with an overall objective of no degradation to the current functional requirements. The current functional requirements of SENS3 are detailed in Section J, Attachment E – Functional Requirements. Offerors are challenged to provide innovative and cost-effective technical, management, and staffing approaches that meet the following objectives.

C.4.1 MANAGE TASK ORDER

a. Provide management, direction, administration, quality control, and leadership of the execution of this TO in accordance with Project Management Institute (PMI) Project Management Body of Knowledge (PMBOK) and Information Technology Infrastructure Library (ITIL) best practices or comparable IT services management (ITSM) framework.
b. Provide effective and transparent communications in performing all work and when addressing issues.
c. Provide a web-based collaborative SENS3 project portal to include functionality for a document library, managing site deployment requests, and a dashboard of the infrastructure status (e.g., key events, incidents, and performance statistics). Distinct but similarly structured and linked portals are required for SENS3 overall (Unclassified), HSDN-specific activities (hosted on HSDN), and C-LAN-specific activities (hosted on

C-LAN). The tool shall be accessible to authorized personnel in DHS, Other Government Agencies (OGAs), and state, local, and tribal partners.

d. Monitor, document, report, and improve management, direction, administration, quality control, and leadership of the execution of this TO.

C.4.2 SENS3 TRANSITION-IN

a. Coordinate and integrate transition activities with the incumbent contractor during a 120-day transition in of SENS3.
b. Coordinate and integrate transition activities with other enterprise service providers.
c. Coordinate and integrate transition activities with users and stakeholders of SENS3.
d. Create a transition-in plan that incorporates the DHS suitability determination process (Entry on Duty (EOD)).
e. Transition the current environment with minimal to no service disruption (see Section J, Attachment Z - Current Service Level Agreements).

C.4.3 SENS3 SERVICE LIFECYCLE

a. Operate and maintain the SENS3 networks in accordance with the Government-approved PWS, Government-approved Service Level Agreements (SLAs), and security policies.
b. Coordinate activities with Government organizations and their contractors responsible for systems that have connectivity with DHS assets within the scope of SENS3 (see Section J, Attachment QQ - Interactions with Other Service Providers).
c. Ensure minimal to no service disruption to the SENS3 networks.
d. Monitor, document, report, and improve the user experience (e.g., service delivery timeline, transparency, self-service options) and service lifecycle planning, implementation, performance, and control.
e. Plan, document, and implement projects (e.g., sites deployments, network migrations, and temporary secure facilities) providing costs, schedule, and status for all projects.

C.4.4 SENS3 CONTINUAL SERVICE IMPROVEMENT (CSI)

a. Provide planning and recommendations for continual improvement of the SENS3 networks to meet or exceed mission-enablement and operational effectiveness and efficiency goals.
b. Research, recommend, and utilize the best of commercially available IT technologies.
c. Improve the user experience.
d. Leverage and coordinate transitions to Intelligence Community Information Technology Enterprise (IC ITE) services with IC ITE services providers and their contractors (see Section J, Attachment J – Notional IC ITE Transition Roadmap).
e. Provide implementation of CSI projects with minimal to no service disruption to the SENS3 networks.
f. Monitor, document, report, and improve CSI planning, implementation, performance, and control.

C.4.5 SENS3 TRANSITION-OUT

a. Coordinate and integrate transition activities with the incoming contractor during a 120-day transition-out of SENS3.
b. Coordinate and integrate transition activities with other enterprise service providers.
c. Coordinate and integrate transition activities with users and stakeholders of SENS3.
d. Maintain minimal to no service disruption to the SENS3 networks during transition-out of SENS3.

C.5 CONSTRAINTS

C.5.1 POLICIES, DIRECTIVES, AND STANDARDS

Existing policies, directives, and standards that are constraining factors for SENS3 requirements include, but are not limited to:

a. DHS Policy 4300B
b. DHS Policy 4300C
c. Committee on National Security Systems Policies (CNSSP) No. 11, “National Policy Governing the Acquisition of Information Assurance and IA-Enabled Information Technology Products.”

C.5.2 FUNDING/APPROPRIATIONS

a. The SENS3 funding environment is complex. HSDN receives annual congressional appropriations to support the Department’s homeland security mission, as well as State and Local Fusion Centers (SLFCs). C-LAN utilizes a working capital fund. Projects are funded by over twenty different customer agencies. Funds have varying expiration dates (e.g. 1-year, multi-year, and no-year) and must often be reviewed and approved by customer agencies’ funding offices before being sent to GSA and added to the contract. This complexity can lead to delays between the final cost estimate for a project and the availability of funding for the contractor to begin the project.